AFFIDAVIT

I, Patrick Hanna, being duly sworn, depose and say:

Introduction

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent charged with enforcing the federal criminal laws and duly authorized by the Attorney General. I am a Special Agent with the Federal Bureau of Investigation (FBI) and currently assigned to the Burlington Resident Agency in Vermont. I have been an FBI Special Agent for fifteen (15) years. My duties as an FBI Special Agent include the investigation of violations of Title 18 of the United States Code as they pertain to corporate fraud, complex financial crimes, embezzlement, public corruption, money laundering and related white collar crimes, as well as violent crimes and criminal enterprises. I have participated in investigations of criminal violations of various federal laws. I have executed search and arrest warrants, interviewed and interrogated subjects, witnesses, and victims, and conducted surveillance. In the course of these investigations, I have gained an understanding of current technology, to include computers and online accounts, and have conducted analyses of the data related to such accounts, for the purpose of solving and proving crimes.

2. I am submitting this Affidavit under Rule 41 of the Federal Rules of Criminal Procedure in support of an Application for a Search Warrant authorizing a search of multiple devices seized in Nevada ("TARGET DEVICES"), more specifically described in Attachment A, and incorporated by reference herein. As discussed more fully below, there is probable cause to believe that individuals associated with Gregory Davis, whose deceased body was discovered on January 7, 2018, committed wire fraud, in violation of 18 U.S.C. § 1343; kidnapping, in violation of 18 U.S.C. § 1201; and murder to obstruct justice, in violation of 18 U.S.C. § 1512(a)(1) (Subject Offenses). There is probable cause to believe that the information described in Attachment B will provide evidence of those crimes. In addition, there is probable cause to believe that the information requested in Attachment B will help identify the person or persons involved in the kidnapping and murder of Mr. Davis.

3. This case is being investigated by the FBI and the Vermont State Police (VSP). Since this affidavit is being submitted for the limited purpose of supporting a search warrant application for the TARGET DEVICES, I have not included details of every aspect of the investigation. Except as otherwise noted, the information contained in this Affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

Probable Cause

A. The Abduction and Shooting

4. On January 7, 2018, VSP responded to a homicide in Barnet, VT. The victim, identified as Gregory Davis, date of birth October 27, 1968, was found partially covered by snow near the base of a snow bank on a pull off area near the west side of Peacham Road. Gregory

Davis was found handcuffed and had been shot multiple times in the head and torso. Davis, it was learned, had resided at 884 Hawkins Road, Danville, VT. Gregory Davis's body was discovered approximately 15 miles from his residence.

5. On the same date, VSP Detectives responded to Davis's home and interviewed his wife, Melissa Davis. Melissa Davis advised VSP Detectives that at approximately 9:00 p.m. on January 6, 2018, a male purporting to be a U.S. Marshal came to the Davis's home. This male had handcuffs, a gun, and was wearing a jacket and mask with an eye opening, both of which had a U.S. Marshals emblem. The male's vehicle had red and blue emergency lights activated on the dash. The male said he had an arrest warrant for Greg Davis for racketeering and that Greg Davis was going to be brought to Virginia.

6. On January 10, 2018, Agent Jennie Emmons confirmed with Supervisory Deputy U.S. Marshal Carl Staley of the Burlington Vermont office of the U.S. Marshals Service that Gregory Davis was not arrested by their agency. Further, it was confirmed by Marshal Staley that there had been no active federal warrants for Gregory Davis.

B. Gregory Davis's Business Dealings

7. Melissa Davis told the VSP Detectives that Davis had been involved in the oil investment business and had concerns about his business partners being involved in fraud. I participated in a follow-up interview with Melissa Davis on January 8, 2018, during which Melissa Davis stated:

a. Melissa Davis and Gregory Davis were married with six children. Melissa Davis is pregnant with the couple's seventh child. Their family has lived in Vermont for approximately three years. At the time of Gregory Davis's death, the family was living at 884 Hawkins Road, Danville, Vermont.

b. Sometime after 2011, Gregory Davis told her that he began working on an oil investment deal with a person named Gregory Gac. Gregory Davis contacted Gac by phone, text, and possibly by email. Gregory Davis told her that he had supply contacts for the oil, and Gac was able to bring in investors. Gregory Davis mentioned that Gac had two specific investors, Serhat and Murat. Melissa Davis understood that Gac had done business with Serhat and Murat before, and they had the means to make the investments.

c. Melissa Davis was told by Gregory Davis that wire transfers had taken place for this investment deal. The first one was for $30,000.00. A receipt was provided by Gac to Gregory Davis showing the wire transfer from Bank of America. Gregory Davis consulted with a lawyer about this wire transfer, and the lawyer told him it was fraudulent. Gregory Davis then contacted Gac and Gac tried to convince Gregory Davis that the deal, and the investors, were legitimate. Three subsequent wire transfers of approximately $10,000.00 each were wired by Gac to Gregory Davis, which appeared to reassure Gregory Davis.

d. Gregory Davis told Melissa Davis that two additional wires transfers occurred later, which came to a TD Bank account for Gregory Davis's company, Mode Commodities. The first one was $40,000.00. The second, more recent transfer, was for $75,000.00. Melissa

understood that the purpose of these wires was for Gac to show Gregory Davis the investors were real and to provide some compensation to Gregory Davis. The Davis family lived off this money, and made some improvements to the 884 Hawkins Road property. Gregory Davis told his wife that he planned to talk to the FBI about the potential fraud matter and that he had told Gac that he was going to the FBI.

e. After the Davis family moved to Vermont, Gregory Davis took a job with a company in Barre, VT called Safety Kleen.

8. On January 9, 2018, Detective Baker also told Agent Emmons that Gregory Davis's cellular phone was located on his body in his left inner coat pocket. The phone is an Apple iPhone, Model A1522, IMEI 359323061224195. According to Melissa Davis, the phone number is 802-377-1303. The service provider for this phone is Verizon. The phone is owned by Safety Kleen. Detective Baker told Agent Emmons that Safety Kleen management provided consent for the search of the phone.

9. Record checks conducted by the employees of the FBI Albany – Burlington Vermont Resident Agency revealed that a Gregory Gac resides at 19705 Chartwell Hill, Excelsior, Minnesota 55331. FBI records show that Gac was interviewed for an FBI investigation regarding an investment fraud matter. The investigation was based in Los Angeles, California, and resulted in the arrest of a person by the name Serhat Gumrukcu in February 2017.

10. On January 9, 2018, Agent Emmons contacted FBI Special Agent Heather Stachnik of the Los Angeles Division. Agent Stachnik advised that she began investigating Serhat Gumrukcu for a real estate investment scheme and a check fraud scheme. She told Agent Emmons the following:

a. During the course of the investigation, she learned that Serhat was involved in additional fraud schemes, to include purporting to be an American doctor who had a special cure for cancer and AIDS, and another involving the oil industry. Serhat is a Turkish national currently living in the USA. Serhat is known to be married to a William Anderson Wittekind.

b. Agent Emmons reviewed a report of a July 7, 2017 interview Agent Stachnik had with Gac. Gac advised he was an escrow agent for Serhat. Gac claimed he met Serhat through a friend of a friend and that Gac wrote the term sheet for an oil investment deal. The investment deal was in an oil trading company with a company called Mode Lauren LLC (hereinafter "Mode"). The investors were Serhat and Murat Gumrukcu, Serhat's older brother. Gac expected to receive residuals from the deal. The Gumrukcus did not make payments as specified in the deal's term sheet and got in arrears with the obligations to Mode. Serhat ended up transferring his interest in Mode to his brother, Murat. Gac was told by a business associate that the Gumrukcus are very wealthy and part of the Turkish royal family. Gac also told Agent Stachnik that he had talked to "Greg Davis" on the phone, but had not met him in person.

c. According to Agent Stachnik, Serhat was charged by the state of California with fraud-related offenses that include his dealings with Gac. He was recently sentenced to five years probation.

11. Current record checks performed by employees of the Albany Division – Burlington Vermont Resident Agency, further identified Serhat Gumrukcu. The records indicate he currently living in West Hollywood, California and uses the cellular telephone number 310-590-8250. The service provider for this phone is T-Mobile.

12. Information obtained from FBI Task Force Officer Jeff Sweeney of Customs and Border Protection show that Murat Gumrukcu, a Turkish national, traveled alone to the United States on December 18, 2017, from Germany to Las Vegas, Nevada. Murat Gumrukcu's I-94 travel record shows a Las Vegas address, 2700 2704 Las Vegas, Las Vegas, NV 89109. CBP system records show that Murat planned to depart from the United States on March 28, 2018 to Turkey.

13. In the course of the FBI Los Angeles investigation regarding Serhat, an additional person by the name of Berk Eratay was identified as having partnered with Serhat in a potential fraud scheme in Las Vegas, in which Serhat introduced a person claiming to be a Saudi Arabian prince to a potential victim. According to record checks performed by FBI Los Angeles, Eratay shows a current address of 2700 Las Vegas Blvd. S, Unit 2704, Las Vegas, Nevada. This appears to be the destination address listed by Murat on his I-94 information.

14. On January 9, 2018, VSP Detective Sergeant Tyson Kinney reviewed text messages on Gregory Davis's phone. Further investigation by other state police personnel showed that Gregory Davis's phone had a contact for a gac@quadfin.com, with the address: 19705 Chartwell Hill, Shorewood, Minnesota, 55331, phone: 612-395-5317, home: 952-470-1969. Gregory Davis had exchanged text messages with Gregory Gac at 612-669-9441 as recently as January 4, 2018.

15. Detective Sergeant Tyson Kinney told Agent Emmons about his review of certain text messages contained on Gregory Davis's phone between what appears to be Gregory Davis and Gac.

a. According to these messages, in summary, it appears Gregory Davis and Gac were involved in a business venture with investors. A contract was in place with the investors. The contract stipulated that if the investors failed to meet their responsibilities, a $75,000 monthly late fee would be levied. As of October 2016, the investors collectively had accrued over $900,000 in late fees. As of October 2016, Gregory Davis was offering several options to Gac to resolve matters with the investors so they could move forward with the business.

b. On December 13, 2017, Gregory Davis texted Gac the following: "Greg, it is always best to square things between people. Goodness when it is the prosecutor's office it's nasty, hard and very unforgiving. Can we agree to seriously work to come to the table this week."

c. On December 27, 2017, Gregory Davis texted Gac: "Happy post Christmas. We need to get things resolved and settled. Please advise as to what they are going to put on the table to accomplish this. Clearly the UBS was just another misrepresenting distraction. It's been duly noted. I look to your reply. GD."

d. On December 28, 2017, Gregory Davis wrote a long text message to Gac, which in summary, showed Greg Davis wished to terminate the business relationship under the terms of the contract or, Greg Davis threatened, the relationship "conversely will end in a series of indictments, clearly bearing civil and criminal repercussions. They are in control of how it ends, but it is the end." From the context of the text messages, "they" appears to refer to Serhat and Murat.

e. On December 29, 2017, Gregory Davis wrote a text message to Gac, demanding a settlement of approximately $980,000 to exit the business deal with Gac, Serhat, and Murat, pursuant to their contract. Further conversation continued at the end of December in which Gac references conversations with Serhat.

f. A final text message to Gac from Gregory Davis, dated January 4, 2018 was located on Gregory Davis's phone which states: "There has now been a history of fraudulent banking documentation that has become the standard. In many instances the banks could not corroborate the claims of the partners. However, in some instances the banks very seriously denied association with the documents and their intention. As regards the TS, all have had a hand in crafting it. Murat himself was directly involved the late sheet segment, to which we gave NO rebuttal. This was then fully executed. We have suffered multiple banking debacles which of itself are VERY serious instances. Therefore, as we've discussed it would be prudent to address the outstanding accounting. Have Murat and Serhat present something to speak to. Let's hopefully close that matter and move forward. Without this our hands will be forced to turn this in to authorities which neither party wants. Please have an honest but serious discussion with the brothers as regards all of the above and let's re-congregate to resolve the immediate matter and discuss how we can move forward. Regards, GD."

16. On January 12, 2018, a search warrant was executed 19705 Chartwell Hill, Excelsior, MN, the residence of Gregory Gac. Gac was also interviewed by me, along with VSP Detectives. Gac stated:

a. Gac owns a company called Quadrant Financial which he runs out of his home in Excelsior, MN. Gac conducts investment business with brothers, Serhat and Murat Gumrukcu. The brothers own a business called Lauran Trading, which is based in Oman. Serhat and Murat have been working successfully with Gac on deals for over three years.

b. Gac met Gregory Davis through other business associates. They have never met in person and have only communicated through phone, text and email. Gac put together an oil-related deal with the Gumrukcu brothers and Gregory Davis. Gac is aware that Gregory Davis has expressed frustration with the Gumrukcu brothers' failure to perform on their obligations in the deal. Gac advised that a third, $40,000, payment is still due to Gregory Davis. A total of three payments, totaling $100,000, were to be paid to Gregory Davis in lieu of the large late fee that had been accrued by the Gumrukcu brothers.

c. Gac advised that in February 2016, Serhat told Gac that Murat was upset that Gregory Davis had called officials at the National Bank of Abu Dhabi to verify that Serhat and Murat maintained accounts there. The bank did not provide an answer to Gregory Davis, but the

brothers learned of this inquiry and Murat was angered because it threatened the brothers' reputations at the bank. During the search warrant at Gac's residence, Gac's notes regarding this matter were located and the notes reflect that Murat was offended.

d. Gac does not believe Gregory Davis and the Gumrukcu brothers have ever met in person though they have talked in conference calls. Gac does not believe Gregory Gac and the Gumrukcu brothers ever spoke directly outside the conference calls.

e. Gac communicates with Murat exclusively through email. Serhat has told Gac that no one is provided with Murat's phone number.

f. According to Gac, while Serhat is the main point of contact for the brothers, Murat is in control of the money.

g. When the interviewers told Gac that Gregory Davis had been murdered, Gac claimed to have no knowledge about the murder.

h. On January 12, 2018, Serhat told Gac that his brother was arranging for the third payment to be made to Gregory Davis, and directed Gac to contact Murat via email about that payment.

17. On January 26, 2018, Agent Emmons spoke to VSP Detective Angela Baker about her review of the contents of Gac's phone, which was seized during the aforementioned search warrant at Gac's residence. According to Detective Baker, Gac's recent texts with Gregory Davis are consistent with those found on Gregory Davis's phone. Further, Detective Baker observed Gac communicated with Serhat at the telephone number 301-590-8250.

a. Detective Baker observed that Gac alerted Serhat to Gregory Davis's discontent with Serhat and Murat. On December 29, 2017, Gac forwarded the aforementioned December 28, 2017 text from Gregory Davis to Gac along to Serhat. In this text, Gregory Davis stated that he believed he has witnessed fraud and alluded to potential civil and criminal repercussions. On prior dates, dating back over a year, Gac summarized in text messages to Serhat, Gregory Davis's anger about the business dealings with the Gumrukcu brothers.

b. In the fall of 2017, numerous texts were sent to Serhat from Gac regarding Gregory Davis's communications with Gac, to include a September 17, 2017 text to Serhat stating, "Gregg is going ballistic, and I don't know if I can control him any more. I heard from Murat that he was returning to Miami today or tomorrow, but nothing specific about meeting. I've heard nothing about meeting with your parents, and nothing from Marc. I'll be getting a call from Gregg soon, and he's going to explode." Further, on September 25, 2017, Gac texted Serhat, stating, "I'm getting nastygrams from Gregg Davis. Anything I can tell him? I'll reach out to UBS shortly" and on October 31, 2017, "...Thanks for pinging Murat. Our friend is all over me again." And, on December 13, 2017, Gac texted Serhat, "Gregg Davis is getting antsy again, and I haven't heard from Murat in four weeks. Gregg wants to see a path forward with ML. With nothing from UBS, I haven misting to tell him. I believe he's on the road to prosecution again, believing there's no future."

18. I have spoken with FBI personnel who have begun reviewing bank records obtained during the investigation, including bank records for a U.S. bank account in Serhat Gumrukcu's name. Those bank records show that between March 2017 and October 2017, Serhat received funds from an unknown Turkish bank account totaling over $220,000. Some of these funds appear to be have funded the payments to Gac and Davis.

19. On February 9, 2018, a search warrant was served on Google for records and information associated with murtagumrukcu@gmail.com and serhat.gumrukcu@gmail.com, which had been identified through Gac directly or Gac's electronic devices. Google returned records related to this warrant on February 28, 2018, some of which have been reviewed. The review of the email messages further corroborate that the Gumrukcu brothers, Gac and Gregory Davis were involved in a business deal, and that Davis was applying pressure on the Gumrukcu brothers by threating to go to the authorities about the Gumrukcus' fraud. Moreover, the emails show that Murat expressed anger at these threats. In late 2015, Murat told Gac that he was finding Gregory Davis's behavior "unacceptable," that he was "highly disturbed" and that he did "NOT wanna hear ridiculous and vulgar threats from him" because his 50k payment was on the way. About two weeks after this email, Murat wrote to Gac, expressing more frustration with Gregory Davis, stating (in part), "As planned, we will initiate this trade to shut him up but I doubt our partnership will survive longer than a couple of lifts … He called me a fraud a second time, there will be no third time. I am trying to clean a mess here and all I hear are threats. . . . If he will harm you or Serhat in any means I will make sure I will find something to return the favor." The records further show that on December 13, 2017, Gac wrote an email message to Murat, in part stating: Gregg Davis again has expressed concern and frustration at the lack of progress and at the absence of firm direction in proceeding toward implementation of the Mode Lauran program. I fear he may pursue a 'nuclear option' if I can't offer him clear guidance on how we are going to move forward."

C. 911 Caller

20. On January 8, 2017, Detective Baker informed Agent Emmons of a suspicious 911 call made near the time and location of Gregory Davis's kidnapping. The VT 911 call center received a call from 802-473-0535 at 8:40 p.m. on January 6, 2018. The 911 call center's technology identified the call as coming from a location on North Danville Road, Danville, VT, only a short distance from the Davis residence.

a. During the call, a male stated that he shot his wife and was going to shoot himself, and gave an address of 71772 Cross Road (with no town information), after which the caller hung up. The call information was relayed to VSP in St. Johnsbury, Vermont. VSP attempted to locate a Cross Road in the St. Johnsbury area without success.

b. VSP thereafter requested that AT&T ping the phone in question due to the exigent circumstance. Several pings were conducted. The ping information showed that the call came from the North Danville Road location. It was learned that the phone was a prepaid phone with AT&T service with no subscriber information available. After the VSP checked the North

Danville location and several possible Cross Roads outside the town of St. Johnsbury, the matter was closed. At that time, Gregory Davis's body had not been discovered.

21. On January 15, 2018, AT&T responded to a search warrant for information associated with the cellular number 802-473-0535, which placed the suspicious call to 911 on January 6, 2018, near the time and location of Gregory Davis's kidnapping.

22. The data provided by AT&T was reviewed by Special Agent James Wines of the FBI's Cellular Analysis Survey Team. After this review, and consultation with AT&T security personnel, Agent Wines advised me that the phone was prepaid phone purchased at a Walmart on January 5, 2018. The records showed only two calls being made by the phone, a four second call to a Pizza Hut in St. Johnsbury, VT at 4:14 p.m. on January 6 and the 911 call at 8:42 p.m. on January 6. The phone used only two sectors of the same cell tower, located in St. Johnsbury, VT, for all cell site activity. Agent Wines also told me that this phone was activated, meaning that it can operate on the network, shortly before 4:00 p.m. on January 6th, within minutes of the Pizza Hut call.

23. On January 16, 2018, Agent Wines advised me that he learned from contacts at Walmart security that the prepaid phone was purchased with $100 cash on January 5, 2018 at 4:14 p.m. at the Walmart located at 100 Supercenter Drive, Clearfield, PA. Agent Wines forwarded numerous security camera images of the individual purchasing the phone, which were obtained from Walmart security. The images show a bearded, adult, white male purchasing the phone. The male arrived and departed in a white Ford Explorer. The camera footage indicates the vehicle parked in the Walmart parking lot around 3:55 p.m. and exited the lot around 4:17 p.m.

24. On January 19, 2018, I learned that FBI personnel in Pennsylvania had canvassed gas stations and other locations in the vicinity of the Walmart at 100 Supercenter Drive, Clearfield, PA, to determine if additional security camera footage of the bearded, white male and/or the white Ford Explorer could be located. Additional video footage of the suspect male and vehicle were located at a BP gas station at 14624 Clearfield Shawville Highway, Clearfield, PA 16830.

25. I reviewed stills of this footage, which included images of the bearded, white male and the white Ford Explorer, and they appear to be the same person and vehicle shown in the Walmart security video. The suspect male purchased gas at the BP station. I saw what appears to be a smartphone in the suspect male's hand. A time stamp on this video put the stop at the gas station in the 4:27 p.m. time period on January 5, 2018. My review of the reports of the agents who travelled to Clearfield, Pennsylvania indicate the display times from the gas station security footage appear to be plus six or seven minutes relative to the actual time. The person depicted in the still images does not appear consistent with photographs obtained of Gac or either Gumrukcu.

26. In early March 2018, I learned from Agent Wines about his review of certain AT&T tower data obtained as a result of search warrants issued by this court in January 2018. Agent Wines received a list of cellular devices connecting to a tower covering the area of Clearfield, Pennsylvania, where the 911 phone was purchased. The data included devices

connecting to the tower at or about the time the 911 phone was purchased. Agent Wines compared this data to data he received listing cellular devices connecting to a tower covering the area of Danville, Vermont, where the abduction took place. The data included devices connecting to the tower at or about the time of Gregory Davis's abduction. Only one cellular phone was common to both sets of data, and it was a device with phone number 201-208-7436 and IMEI number 86423703243563. Further investigation by Agent Wines determined that the device that connected to towers in Pennsylvania and Danville, Vermont, is an Android cell phone purchased in a Walmart in Oak Grove, Missouri on November 13, 2017 and additional service (minutes/data) for that phone was purchased at a Walmart in Dexter, Missouri on January 4, 2018. Agent Wines obtained receipts for these purchases, which show these purchases, like the 911 cell phone purchase in Pennsylvania on January 6, 2018, were made with $100 cash. The details on the receipt suggest that the customer paid with a $100 bill for all three purchases. I obtained a search warrant for historical location information for this phone on March 2, 2018, from this Court. Agent Wines has told me that he has begun to review this historical location information and that the phone used data between January 4, 2018 and January 6, 2018, and that the phone appears to be have been turned off or not used shortly after the time of the abduction. Agent Wines has also told me that Android phones are typically associated with a Google account and the data reviewed shows that the phone connected on multiple occasions to Google services.

D. Identification of Devices to be Examined

27. The TARGET DEVICES, more fully described in Attachment A, were seized by the Las Vegas office of the FBI. Special Agent Christopher McPeak provided me the following information.

a. On March 16, 2018, members of the Las Vegas Division Violent Criminal Threat Squad executed a federal search warrant at 2700 Las Vegas Boulevard South #2704, Las Vegas, Nevada. Following this search, a 2018 Toyota Yaris SUV was searched pursuant to a federal search warrant. The search warrants were authorized by US Magistrate Judge George W. Foley, Jr. on March 12, 2018. The search of the apartment commenced at approximately 12:10 p.m. and concluded at approximately 1:00 pm. The search of the vehicle commenced at approximately 1:10 pm and concluded at approximately 1:30 p.m. The TARGET DEVICES were seized in these two searches. The Nevada warrants authorized the seizure of devices but did not explicitly describe the items to be searched on those devices. I seek this warrant to authorize more precise direction concerning data to be searched for on the devices.

b. Murat Gumrukcu was present during the service of the search warrant. Agent McPeak interviewed Gumrukcu in the security office of the Sky Las Vegas condominium building. Gumrukcu agreed to speak with Agent McPeak on a voluntary basis. Agent McPeak made it clear that Gumrukcu could stop the interview at any time and go back to his apartment.

c. Gumrukcu stated he saw his brother Serhat Gumrukcu two times since arriving in the United States on a tourist visa, once when he initially arrived in December of 2017 and again on January 1, 2018. Gumrukcu stated he communicates with his brother Serhat via telephone,

text, and WhatsApp messenger. Gumrukcu could not recall the phone number for any of the three seized phones.

d. Gumrukcu indicated he was familiar with Gregory Gac through his brother Serhat. He understood Gac to be an older banker who worked with his brother Serhat. Gumrukcu was unable to describe or identify what business his brother Serhat had with Gac. Gumrukcu denied ever communicating or meeting directly with Gac. When Gumrukcu was asked why the FBI possessed evidence that Gumrukcu had communicated with Gac, Gumrukcu said that he did not know, but he did not communicate with Gac. Gumrukcu was not aware of the fact that "one of" Gac's business partners had "died."

Definitions

28. The following non-exhaustive list of definitions applies to this Affidavit and its Attachments:

a. "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices. Digital device also includes computers, as defined pursuant to 18 U.S.C. § 1030(e)(1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. "Computer hardware" consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, mobile telephones, video gaming devices, portable electronic music players, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. "Wireless telephone" (or mobile telephone, or cellular telephone, or iPhone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic

"address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer passwords, pass-phrases, and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber.

h. "ISP Records" are records maintained by ISPs pertaining to their subscribers, and may include account application information, subscriber and billing information, account access information (often in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISPs' servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data.

i. "Internet Protocol address" or "IP address" refers to an identifier used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP often assigns a different IP address to a subscriber's modem when it accesses the Internet. IP addresses might also be static, that is, an ISP assigns a subscriber's modem a particular IP address that does not change.

j. "Electronic communications system" refers to any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for electronic storage of such communications.

k. "Electronic Communications Service Providers" (ECSPs) are commercial organizations which provide individuals and businesses the ability to send or receive wire or electronic communications.

l. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies, pictures), mechanical form (including, but not limited to, phonograph records, printing, typing) or electronic or magnetic form (including, but not limited to, tape recordings, storage devices such as flash storage devices [such as SD cards, compact flash, USB flash drives, etc.], floppy disks, hard drives, CD-ROMs, digital video disks (DVDs), PDAs, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device). These terms also include any applications (e.g. software programs). The term "communications" expressly includes, among other things, emails, instant messages, chat logs, correspondence attached to emails (or drafts).

m. "Imaging" or "copying" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents but attributes may change during the reproduction.

n. "Hash value," or "SHA-1," refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. Secure Hash Algorithm Version 1, or SHA-1, is a mathematical algorithm. SHA-1 was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA). The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. It is computationally infeasible (2^160th) to find two different files that produce the same SHA-1 value. This allows investigators to identify a file by the value, regardless of the name of the file beyond 99.99 percent certainty. The SHA-1 digital signature can be explained as a digital fingerprint, or DNA of the file.

Background Regarding Digital Devices

29. Based upon my training and experience, and my discussions with other law enforcement officials, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures or documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, one terabyte (TB) hard drives are not uncommon in computers. As a rule of thumb, users with one gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 500 million pages, that, if printed, would fill six 35' x 35' x 10' rooms. Similarly, a one TB drive could contain 900 full run movies, or 900,000 songs, or four million images. With digital devices, users can store data for years at little cost to no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for many years, been encouraged to never delete their emails. For example, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." *See* Bill Kee, *Welcome to Official Gmail Blog*, https://gmail.googleblog.com/2007/06/welcome-to-official-gmail-blog.html (July 3, 2007); *see also* Rob Siembroski, *More Gmail Storage Coming For All*, https://gmail.googleblog.com/2007/10/more-gmail-storage-coming-for-all.html (Oct. 12, 2007) (promoting its "Infinity+1" plan to constantly give subscribers more storage).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing purposes or email headers may automatically list the servers which transmitted the email. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user's history of websites visited so users can more easily re-access those sites. Browsers also temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is practically resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple locations, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the

recycle bin, the data does not actually disappear; rather it remains in "free space" or "slack space" (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a "recovery" or "swap file." Fourth, files from websites are automatically retained in a temporary cache which is only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

Specifics of Searches and Seizures of Digital Devices

30. Based on my training, my experience, and information provided to me by those involved in the forensic examination of digital devices including cell phones, I know that completely segregating information before an examiner has started reviewing digital evidence is inconsistent with the evidence assessment process. This is true for the following reasons:

a. This application seeks permission to locate and seize not only data that might serve as direct evidence of the Subject Offenses, but also for evidence that establishes how digital devices were used, the purpose of their use, and who used them. Additionally, this application seeks information about the possible location of other evidence.

b. This application seeks permission to search and seize evidence, fruits, or instrumentalities found in the devices described in Attachment A. Some of these items may be files and other data that is generated by a user (e.g. documents, pictures, and videos). Alternatively, other items may be device generated data that becomes meaningful only upon forensic analysis. For example, as noted, a hard drive may contain records of how a computer was used, the purposes for which it was used, and who has used these records. These items are the subject of this warrant.

c. For instance, based upon my training, my experience, and information provided by others involved in the forensic examination of digital devices, I know the following: First, as noted, data that is not currently associated with any file can provide evidence of a file that once existed, but which has since been deleted or altered. This can include a deleted portion of a file (e.g. a paragraph deleted from a document). Second, applications such as web browsers, email, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Third, operating systems can record information, such as the attachment of peripherals (e.g. USB flash drives), and the times the device was in use. Similarly, file systems record the dates files were created and the sequence in which they were created. Any of this information may be evidence of a crime, or indicate the existence and location of evidence in other locations on the digital device.

d. In determining how a digital device has been used, the purpose for which it was used, and who has used it, it is sometimes necessary to establish that a particular thing is not present. For example, in cases where more than one person has used a digital device, agents can infer that a defendant must have been the person who used that device to commit a crime by eliminating the possibility that other people used that device during that time. Because file systems often list the dates and times those files were created, this information can help exclude the possibility that other people were using that digital device. As another example, by reviewing a

computer's Index.dat files (a system file that keeps track of activity conducted in Internet Explorer), a forensic examiner can determine whether a user accessed other information close in time to the file creation dates, times, and sequences so as to establish user identity and exclude others as having used that computer during times related to the criminal activity. Demonstrating the significance of the absence of certain data on a digital device may require analysis of the digital device as a whole.

e. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a user or excluding a user. All of these types of evidence may indicate ownership, knowledge, and intent.

f. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

31. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

32. Based on my training, my experience, and information given to me by others involved in the forensic examination of digital devices, I know that searching for this kind of evidence involves technical, complex, and dynamic processes, which may require expertise, specialized equipment and a knowledge of how digital devices are often used to commit the Subject Offenses.

33. Because these warrants seek only permission to examine devices already in law enforcement's possession, the execution of these warrants does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

Dated at Burlington, in the District of Vermont, this 5th day of April 2018.

Patrick Hanna
Special Agent, FBI

Sworn to and subscribed before me this 5th day of April 2018.

Honorable John M. Conroy
United States Magistrate Judge